

### **REMARKS**

Claims 11, 13, 14, 16-19, and 22-28 are pending. The Examiner's reconsideration of the rejection in view of the remarks is respectfully requested.

Claims 11, 13, 14, 16, 18 and 22-26 have been rejected under 35 U.S.C. 102(b) as being unpatentable over Sudia et al. (USPAN 2001/0050990). The Examiner stated essentially that Sudia teaches all of the limitations of Claims 11, 13, 14, 16, 18 and 22-26.

Claims 11, 22 and 23 are the independent claims.

Claims 11 and 22 claim, *inter alia*, “reading a certificate including a first public key into a protected memory; validating said certificate with a second public key permanently stored on said processor; reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected; preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key.” Claim 23 claims, *inter alia*, “a processor in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in ~~of~~ said signed authorized code is original in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor.”

Sudia teaches a cryptographic system with a key escrow feature (see Abstract). Sudia does not teach “preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first

public key” as claimed in Claims 11 and 22 nor “a processor... verifying that a digital signature contained in ~~of~~ said signed authorized code is original in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor” as claimed in Claim 23. Sudia teaches that new or additional firmware code is signed using a manufacturer’s signature. Sudia teaches that the device verifies the manufacturer’s signature using the public signature key of the manufacturer (see paragraph [0248], second to last sentence). Respectfully, the manufacturer’s signature of Sudia is not analogous to the claimed first public key. That is, Sudia does not teach that the manufacturer’s signature is used to verify a digital signature of code; the function of verification is performed in every instance using with the public signature key of the manufacturer. Thus, Sudia does not teach the validation of a first public key using the public signature key of the manufacturer, the first key which is then used for verifying digital signatures, essentially as claimed. Therefore, Sudia fails to teach all the limitations of Claims 11, 22 and 23.

Referring to the Response to Arguments; respectfully, the Examiner’s Response relies on the injection of “a public key of the third party firmware provider...” Respectfully, the reliance on subject matter outside the express teachings of the Sudia reference (to teach all the limitations of Claims 11, 22, and 23) goes outside the scope of a rejection under 35 USC 102. Further, the rationale is contrary to the express teachings of Sudia, which provides that a system “uses modern public key certificate management, enforced by a chip device that also self-certifies” (see Abstract). That is, any secondary key, such as “a public key of the third party firmware provider...”, is contrary to the teachings of Sudia. Such a secondary key as proposed in the Response to Arguments would seriously compromise the intended function of Sudia to avoid reliance on cryptosystems and digital signatures (see paragraph [00061]).

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. Claims 15, 20 and 21 have been cancelled. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 17, 19, 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Sudia and Morgan teach or suggest all of the limitations of Claims 17, 19, 27 and 28.

Claims 17 and 19 depend from Claim 11. Claims 27 and 28 depend from Claim 23. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Reconsideration of the rejection is respectfully requested.

For the forgoing reasons, the application, including Claims 11, 13, 14, 16-19, and 22-28, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: April 8, 2008

By: /Nathaniel T. Wallace/  
Nathaniel T. Wallace  
Reg. No. 48,909  
Attorney for Applicants

**F. CHAU & ASSOCIATES, LLC**  
130 Woodbury Road  
Woodbury, New York 11797  
TEL: (516) 692-8888  
FAX: (516) 692-8889